

Organizations can use the Barracuda Load Balancer to enhance the scalability and availability of their Microsoft Office Communications Server deployments.

## Office Communications Server Overview

Organizations use solutions like Microsoft Office Communications Server to allow them to effectively disseminate information and enhance collaborative efforts among their employees. Microsoft Office Communication Suite offers functionality such as VoIP, instant messaging and Web collaboration. All these services may be utilized by clients from either the internal office network or from the Internet.

Companies deploying Microsoft Office Communication servers for higher traffic throughput look to deploy a scalable solution. To scale the deployment of the Microsoft Office Communication Server solution, Microsoft recommends using a hardware load balancer to distribute the traffic among multiple OCS servers.

Barracuda Networks has conducted interoperability tests between the Barracuda Load Balancer and Office Communications Server 2007 R2 (OCS). This document describes some ways to deploy the Barracuda Load Balancer to provide scaling in an OCS environment.

## Prerequisites

- Microsoft Office Communications Server 2007 R2 Enterprise Edition
- Barracuda Load Balancer running firmware version 3.3.1.005 or higher
- Barracuda Load Balancer model 340 or above is required
- *For Internal Office Communications Deployment:* Minimum one Barracuda Load Balancer, two recommended for high availability
- *For both Internal Office Communications Deployment and Edge Deployment:* Minimum two Barracuda Load Balancers, four recommended for high availability.
- *For Internal Office Communications Deployment, Edge Deployment, and Communicator Web Access Deployment:* Minimum three Barracuda Load Balancers, six recommended for high availability.

This document assumes that you have installed your Barracuda Load Balancer(s), have connected to the Web Interface, and activated your subscription(s). If you are planning to deploy Office Communications Server with high availability, you must first cluster your Barracuda Load Balancers. See the [Barracuda Load Balancer Administrator's Guide](#) for assistance with these steps.

## Additional References

- [Barracuda Load Balancer Administrator's Guide:](#)
  - <http://www.barracudanetworks.com/documentation/>
- Technet Article on Load Balancing Enterprise Pools:
  - <http://technet.microsoft.com/en-us/library/bb870398.aspx>
  - [http://technet.microsoft.com/en-us/library/dd572362\(office.13\).aspx](http://technet.microsoft.com/en-us/library/dd572362(office.13).aspx)
- Technet Article on Load Balancing Edge Servers with Enterprise Pools:
  - <http://technet.microsoft.com/en-us/library/bb870418.aspx>

- Technet Article on Using a Load Balancer to Increase Capacity and Availability with Communicator Web Access
  - [http://technet.microsoft.com/en-us/library/dd441196\(office.13\).aspx](http://technet.microsoft.com/en-us/library/dd441196(office.13).aspx)

## Terminology

The following table lists some of the terms used in this document.

**Table 1. Terminology**

Definitions	
Front-End Server	An OCS server in the internal network.
Edge Server	An OCS server deployed in the perimeter network.
Fully Qualified Domain Name (FQDN)	The unique name for a specific computer or host that can resolve to an IP address, e.g. <code>www.example.com</code>
Service	A combination of a virtual IP (VIP) address and one or more TCP/UDP ports that the Barracuda Load Balancer listens on. Traffic arriving over the specified port(s) is directed to one of the Real Servers associated with a particular Service.
OCS	Office Communications Server
CWA	Communicator Web Access

## Deployment Options

The supported deployments of the Office Communications Server and the Barracuda Load Balancer are described in the following sections.

### ***OCS Front-End Server Deployment Options***

Servers in an Office Communications Server enterprise pool communicate with each other using the VIP address of the pool. To facilitate this communication, create a TCP Proxy Service and associate the servers with it. The servers and the Barracuda Load Balancer must be deployed using a **one-armed** topology in either a single or multiple subnet configuration.

Deploying internal OCS pools using a two-armed topology (Route-Path), Direct Server Return (DSR) or Bridge Mode **does not work**.

### ***OCS Edge Server Deployment Options***

Load balanced Edge deployments are supported using either a **one-armed** topology using a TCP Proxy Service or a **two-armed** (Route-Path) topology using a Layer 4 Service.

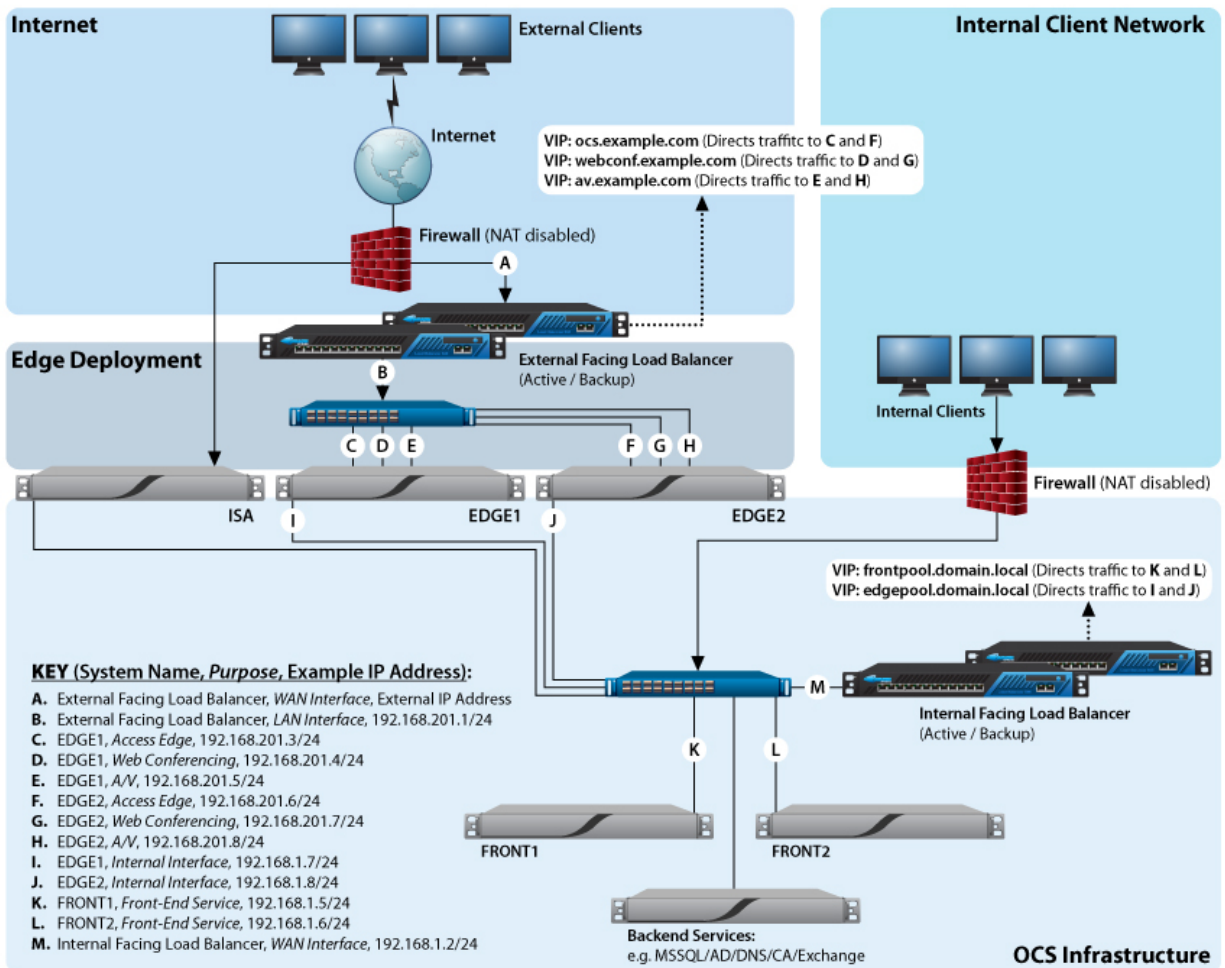
Bridge Mode and Direct Server Return deployments **do not work**.

## Deployment Example

Figure 1: OCS Deployment Example shows an example of a complete Office Communications Server deployment with Barracuda Load Balancers. This example is used in the deployment tasks that are detailed in the next sections.

Note that in this example, the Edge deployment uses a Route-Path topology while the Front-End deployment uses a one-armed topology.

Figure 1: OCS Deployment Example



As shown in the diagram, the firewall should not NAT inbound traffic addressed to the Edge deployment.

## Deployment Tasks

To deploy the Barracuda Load Balancer in an Office Communications Server environment, complete the following tasks using the instructions in the rest of this document.

**Table 2. Deployment tasks**

Task	Where
1. Modify TCP and UDP Connections Settings	Do this on all active Barracuda Load Balancers, both internal and external. If your systems are clustered, the passive systems do not need to be configured separately.
2. Configure Enterprise Pool Services.	Do this on the internal-facing Barracuda Load Balancers.
<b>If you have an edge deployment you must also do the following tasks:</b>	
3. Configure Internal Edge Services.	Do this on the internal-facing Barracuda Load Balancers.
4. Configure External Edge Services.	Do this on the external-facing Barracuda Load Balancers.
5. Confirm the Configure Edge Server Wizard Setting.	Check this on all Edge Servers.
<b>If you have deployed Director servers you must also do the following task:</b>	
6. Configure Director Services.	Do this on the Director Barracuda Load Balancers.
<b>If you have deployed Communicator Web Access you must also do the following task:</b>	
7. Configure Communicator Web Access Services.	Do this on the CWA Barracuda Load Balancers.

**Note:** If your Barracuda Load Balancers are clustered, the configuration between the active and passive systems is synchronized. There is no need to modify any passive Barracuda Load Balancers.

### 1. Modify TCP and UDP Connections Settings

Do this on all active Barracuda Load Balancers, both internal (the Barracuda Load Balancer configured with the Front-End servers) and external (if there is a Barracuda Load Balancer deployed with Edge servers).

The Barracuda Load Balancer comes configured with default settings that work with most applications. Office Communications Server requires changes to the default advanced IP settings on the Barracuda Load Balancer to ensure it complies with Microsoft's specifications.

**To modify the TCP and UDP Connections settings on the System Settings page:**

- 1.1. Go to the **Advanced > System Settings** tab in the Web interface.
- 1.2. In the **TCP Connections Timeout** box, enter 1800 (30 minutes).
- 1.3. In the **UDP Connections Timeout** box, enter 1800 (30 minutes).

## 2. Configure Enterprise Pool Services

Do this on the internal-facing Barracuda Load Balancers.

To configure all the Services needed for an internal OCS deployment, perform the following steps on the internal-facing Barracuda Load Balancer:

- 2.1. Go to the **Basic > Services** page in the Web Interface.
- 2.2. For each entry in the following tables, add a Service. To add a Service:
  - In the **Service Name** box, enter the name for the Service.
  - In the **Virtual IP Address** box, enter the IP address for the FQDN of your Internal OCS Pool.
  - Select the protocol and in the **Port** box, enter the port for the Service in the table.
  - In the **Real Servers** box, enter the IP address for every Front-End server in your OCS Pool.
- 2.3. All of the Services in Table 3 are **required**. Add each Service in Table 4 only if you have deployed that feature.

**Table 3. Required Services for internal OCS deployment**

Service Name	Virtual IP Address	Protocol	Port	Real Servers
MTLS Front	IP for FQDN of Internal Enterprise OCS Pool e.g.192.168.1.11/24 for frontpool.domain.local	TCP	5061	IP Addresses of your Front-End servers (K and L from the example)
DCOM WMI Front	IP for FQDN of Internal Enterprise OCS Pool	TCP	135	IP Addresses of your Front-End servers (K and L from the example)
Internal Conf Front	IP for FQDN of Internal Enterprise OCS Pool	TCP	444	IP Addresses of your Front-End servers (K and L from the example)
HTTPS Front	IP for FQDN of Internal Enterprise OCS Pool	TCP	443	IP Addresses of your Front-End servers (K and L from the example)



The Services in the following table are **optional**. Add only those Services that correspond to a feature that you have deployed.

**Table 4. Optional Services for internal OCS deployment**

Service Name	Virtual IP Address	Protocol	Port	Real Servers
Application Sharing (optional)	IP for FQDN of Internal Enterprise OCS Pool	TCP	5065	IP Addresses of your Front-End servers (K and L from the example)
QoE Agent (optional)	IP for FQDN of Internal Enterprise OCS Pool	TCP	5069	IP Addresses of your Front-End servers (K and L from the example)
Response Group Service (optional)	IP for FQDN of Internal Enterprise OCS Pool	TCP	5071	IP Addresses of your Front-End servers (K and L from the example)

**Table 4. Optional Services for internal OCS deployment**

Service Name	Virtual IP Address	Protocol	Port	Real Servers
Conferencing Attendant (optional)	IP for FQDN of Internal Enterprise OCS Pool	TCP	5072	IP Addresses of your Front-End servers (K and L from the example)
Conferencing Announcement (optional)	IP for FQDN of Internal Enterprise OCS Pool	TCP	5073	IP Addresses of your Front-End servers (K and L from the example)
Outside Voice Control (optional)	IP for FQDN of Internal Enterprise OCS Pool	TCP	5074	IP Addresses of your Front-End servers (K and L from the example)

- 2.4. For each Service created, edit the Service by clicking the **Edit**  graphic next to the Service entry in the table. On the **Service Detail** page that appears:
- In the **General** section, set the Service Type to **TCP Proxy**.
  - In the **Advanced Options** section, set **Session Timeout** to 0 (session never times out).
- 2.5. For the DCOM WMI Front Service only, edit each Real Server associated with the Service by clicking the **Edit**  graphic next to each Real Server entry in the table. On the **Real Server Detail** page that appears:
- In the **Server Monitor** section, set the **Testing Method** to **TCP Port Check**.
  - In the **Port** field, enter the value **5061**. It is better to test port 5061 for this Service because port 135 always passes the TCP port check, even if OCS Services are not responding.

### 3. Configure Internal Edge Services

Do this on the internal-facing Barracuda Load Balancers.

**To configure all the Services needed for a load balanced OCS Edge deployment, perform the following steps on the internal-facing Barracuda Load Balancer:**


- 3.1. Go to the **Basic > Services** page in the Web Interface.
- 3.2. For each entry in Table 5, add a Service. In the **Service Name** box, enter the name for the Service. In the **Virtual IP Address** box, enter the IP address for the FQDN of your Internal Edge OCS Pool. In the **Port** box, enter the port for that Service in the table. In the **Real Servers** box, enter the internal IP address for every Edge server.

**Table 5. Services for OCS Edge deployment on the internal-facing Barracuda Load Balancer**

Service Name	Virtual IP Address	Protocol	Port	Real Server
MTLS Edge	IP for FQDN of Internal Edge Enterprise OCS Pool e.g.192.168.1.12/24 for edgepool.domain.local	TCP	5061	Internal IP addresses of your Edge Servers (I and J from the example)
AV Auth Edge	IP for FQDN of Internal Edge Enterprise OCS Pool	TCP	5062	Internal IP addresses of your Edge Servers (I and J from the example)

**Table 5. Services for OCS Edge deployment on the internal-facing Barracuda Load Balancer**

Service Name	Virtual IP Address	Protocol	Port	Real Server
RTP HTTP Edge	IP for FQDN of Internal Edge Enterprise OCS Pool	TCP	443	Internal IP addresses of your Edge Servers (I and J from the example)
WebConf Edge	IP for FQDN of Internal Edge Enterprise OCS Pool	TCP	8057	Internal IP addresses of your Edge Servers (I and J from the example)
RDP Media Edge	IP for FQDN of Internal Edge Enterprise OCS Pool	UDP	3478	Internal IP addresses of your Edge Servers (I and J from the example)

- 3.3. For each **TCP** Service created, edit the Service by clicking the **Edit**  graphic next to the Service entry in the table. In the **General** section, set the Service Type to **TCP Proxy**. In the **Advanced Options** section set **Session Timeout** to 0 (session never times out).
- 3.4. No change is required for RDP Media Edge, which is a **UDP** Service.

## 4. Configure External Edge Services

Do this on the external-facing (Internet-facing) Barracuda Load Balancers.

The Real Servers should be physically connected to a switch which is connected to the LAN port of the Barracuda Load Balancer.

**To configure all the Services needed for a load balanced Edge Deployment of Office Communications Server, perform the following steps on the external-facing Barracuda Load Balancer:**

- 4.1. Go to the **Basic > Services** page in the Web Interface.
- 4.2. For each entry in the Table 6, add a Service. In the **Service Name** box, enter the name for the Service. In the **Virtual IP Address** box, enter the IP address for the FQDN of your Internal Edge OCS Pool. In the **Port** box, enter the port for that Service in the table. In the **Real Servers** box, enter the internal IP address for every Edge server.

**Table 6. Services for load balancing Edge Deployment of OCS**

Service Name	Virtual IP Address	Protocol	Port	Real Server
Access Edge	IP for FQDN of Access Edge e.g. IP address for ocs.example.com	TCP	443	IP address of Access Edge NICs on each Edge Server (C and F from the example)
WebConf Edge	IP for FQDN of WebConf Edge e.g. IP address for webconf.example.com	TCP	443	IP address of WebConf NICs on each Edge Server (D and G from the example)

**Table 6. Services for load balancing Edge Deployment of OCS**

Service Name	Virtual IP Address	Protocol	Port	Real Server
AV Edge	IP for FQDN of AV Edge e.g. IP address for av.example.com	TCP	443	IP address of AV NICs on each Edge Server (E and H from the example)
AV UDP Edge	IP for FQDN of AV Edge e.g. IP address for av.example.com	UDP	3478	IP address of AV NICs on each Edge Server (E and H from the example)

No modifications need to be made to the default settings for these Services.

## 5. Confirm the Configure Edge Server Wizard Setting

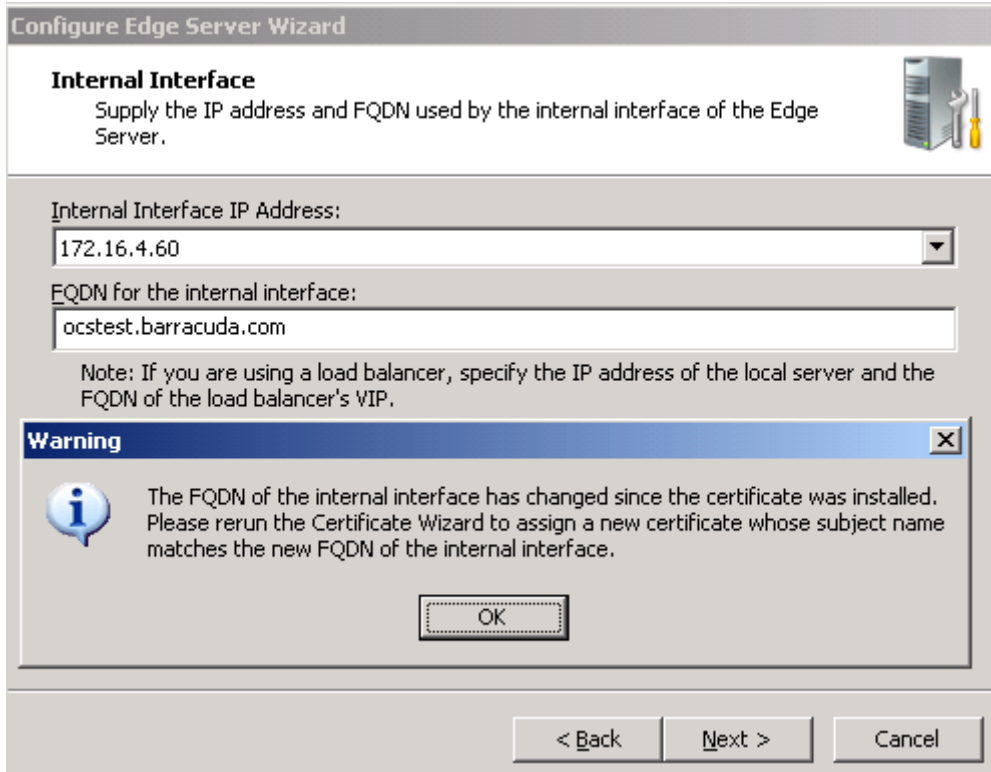
Check this on all Edge Servers.

When completing the **Configure Edge Server Wizard** you will see the **Internal Interface** dialog. The following note is displayed: "If you are using a load balancer, specify the IP address of the local server and the FQDN of the load balancer's VIP." In the **FQDN for the internal interface** box, enter the FQDN for the Access Edge DNS entry that external users will use.

If this is set correctly, then when the Edge Servers are queried for their host name strings, they will return the FQDN of the VIP address for the external Access Edge instead of the FQDN of the internal interface. This ensures that the SAN (Subject Alternative Name) on the certificate assigned to this internal interface for the Access Edge matches the Edge server's host string.

See *Figure 2: Configure Edge Server Wizard* for a screen shot of the wizard.

**Figure 2: Configure Edge Server Wizard**



## 6. Configure Director Services


Do this on the Director Barracuda Load Balancers.

**To configure all the Services needed for Director Services, perform the following steps on the Director Barracuda Load Balancer:**

- 6.1. Go to the **Basic > Services** page in the Web interface.
- 6.2. For each entry in the Table 7, add a Service. In the **Service Name** box, enter the name for the Service. In the **Virtual IP Address** box, enter the IP address for the FQDN of your Director Service. In the **Port** box, enter the port for that Service in the table. In the **Real Servers** box, enter the IP address for every Director server.

**Table 7. Services for load balancing Director Services**

Service Name	Virtual IP Address	Protocol	Port	Real Servers
Director MTLS	IP for FQDN of the Director Service	TCP	5061	IP addresses of your Director Servers
Director MTLS Legacy	IP for FQDN of the Director Service	TCP	5060	IP addresses of your Director Servers

- 6.3. For each Service created, edit the Service by clicking the **Edit**  graphic next to the Service entry in the table. On the **Service Detail** page that appears:

- In the **General** section, set the Service Type to **TCP Proxy**.
- In the **Advanced Options** section, set **Session Timeout** to 0 (session never times out).

## 7. Configure Communicator Web Access Services

Do this on the Communicator Web Access Barracuda Load Balancers.

Communicator Web Access (CWA) is an optional feature of Office Communication Server that allows users who do not have access to the Office Communicator Client to access many of the features of Office Communications Server from a browser. Installations of CWA that have greater than 5000 users should deploy a load balancer for this feature. Microsoft recommends that you dedicate one or more load balancers that are used only for CWA for acceptable performance.

Configure the CWA servers to use HTTP rather than HTTPS. This allows the Barracuda Load Balancer to do SSL offloading, which improves the performance of the CWA Service. Also, this allows end user connections to be maintained using cookies, as recommended by Microsoft.



**To configure the Services needed for a load balanced Communicator Web Access Server, perform the following steps on the Communicator Web Access Barracuda Load Balancer:**


- 7.1. Go to the **Basic > Certificates** page and upload the CWA certificate to the Barracuda Load Balancer.
- 7.2. Go to the **Basic > Services** page in the Web Interface.

Add a Service for each entry in the Table 8. In the **Service Name** box, enter the name for the Service. In the **Virtual IP Address** box, enter the IP address for the FQDN of your CWA Service. In the **Port** box, enter 443. In the **Real Servers** box, enter the internal IP address for every CWA server.

**Table 8. Service for load balancing Communicator Web Access Servers**

Service Name	Virtual IP Address	Protocol	Port	Real Server
CWA	IP for FQDN of CWA e.g. IP address for cwa.domain.local	TCP	443	IP address of CWA Servers

- 7.3. Edit the Service by clicking the **Edit**  graphic next to the Service entry in the table.
  - a. In the **General** section, set the Service Type to **Layer 7 - HTTP**.
  - b. In the **Service Monitor** section, in the **Testing Method** list, click **HTTP**. In the **Test Target** box, enter `http://<fqdn of your CWA website>/` For example, `http://cwa.domain.local/`
  - c. In the **Test Match** box, enter **Microsoft Corporation**.
  - d. In the **Persistence** section, change the **Persistence Type** option button to **HTTP Cookie**.
  - e. In the **SSL Offloading** section, change the **Enable HTTPS/SSL** option button to **Yes**. In the **SSL Certificate** list, select the name of the certificate you uploaded for CWA.
  - f. In the **Advanced Options** section set **Session Timeout** to 0 (session never times out).
- 7.4. For each Real Server added, edit the Real Server by clicking the **Edit**  graphic next to each Real Server entry in the table. In the **Real Server Detail** section, change the value for **Port** to 80

- 7.5. Go to the **Advanced > URL Rewrites** page in the Web interface and create a rule to replace outgoing `http://<fqdn of your CWA Web site>` with `https://<fqdn of your CWA Web site>`. This rewrites absolute paths written by CWA so that they all appear as encrypted links. This rule prevents unsecure content errors in the browser.
- In the **Layer 7 – HTTP Services** section, select the CWA Service from the list.
  - In the **Response Body Rewrite** section, create a new rule with the following options:
    - Rule Name: `cwa`
    - Rule Order: `1`
    - Host Match: `<fqdn of your CWA Web site>`, e.g. `cwa.domain.local`
    - URL Match: `/cwa/client/*`
    - Search String: `http://<fqdn of your CWA Web site>`, e.g. `http://cwa.domain.local`
    - Replace String: `https://<fqdn of your CWA Web site>`, e.g. `https://cwa.domain.local`
- 7.6. Create the CWA Redirect Service. This Service ensures that end users are redirected from HTTP to the HTTPS Service.
- Go to the **Basic > Services** page in the Web interface.
  - In the **Service Name** box, enter the name for the CWA Redirect Service. In the **Virtual IP Address** box, enter the IP address for the FQDN for your CWA Service. Select the protocol TCP. In the **Port** box, enter `80`.
- 7.7. Edit the CWA Redirect Service by clicking the **Edit**  graphic next to the Service entry in the table.
- In the **General** section, set the Service Type to **Layer 7 - HTTP**.
  - Set **Enable HTTP Redirect** to **Yes**.
- 7.8. Test the CWA installation.
- Open a browser and enter: `https://<fqdn of your CWA Web site>`, e.g. `https://cwa.domain.local`
  - Ensure that all images load and that you are able to log into the CWA application without errors.

Your installation is now complete.